Exhibit B

GOODWIN

Robert D. Carroll
+1 617 570 1753
RCarroll@goodwinlaw.com

Goodwin Procter LLP
100 Northern Avenue
Boston, MA 02210

goodwinlaw.com
+1 670 570 1000

December 19, 2024

BY EMAIL & FEDEX

Jonathan Hershon
CEO, Pathway Medical, Inc.
jonathan@pathway.md
contact@pathway.md
253 Av. Laurier O
Montréal, QC H2V 2K1 Canada

Re: ***Cyberattack by Pathway against OpenEvidence***

Dear Mr. Hershon,

This firm represents Xyla Inc., d/b/a OpenEvidence ("OpenEvidence").

It has come to the attention of our client that Pathway Medical, Inc. ("Pathway"), together with its cofounders and most senior executives—including yourself and your co-founder and Louis Mullie—have illegally conducted at least two hundred cyber-attacks against OpenEvidence. These attacks include "prompt injection" hacking techniques, which have targeted OpenEvidence's protected, confidential, and trade secret code and information, including, but not limited to OpenEvidence's System Prompt code, in violation of a number of U.S. federal and state laws (as well as OpenEvidence's terms of use).

These unlawful activities have caused and threaten to cause significant economic and competitive harm to OpenEvidence, and they have been undertaken intentionally and clandestinely (including, as presently known to OpenEvidence, through Pathway employees illegally impersonating medical professionals to gain illegal access to OpenEvidence's systems and proprietary information). In addition, as presently known to OpenEvidence, Pathway's illegal conduct has been advanced by you individually as well as several other employees and agents of Pathway, including your cofounders. Pathway and those acting on its behalf may be held jointly and severally liable for money damages resulting from any and all harm caused to OpenEvidence, including punitive damages for willful and malicious conduct, stemming from Pathway's illegal access of OpenEvidence's AI information platform.

The misconduct of Pathway and its employees and agents includes, but is not limited to, attempting to circumvent OpenEvidence's protective technological measures associated with its services by impersonating medical professionals, fraudulently using National Provider Identifiers ("NPIs") or falsifying NPIs, illegally accessing computer systems using these fraudulent and/or falsified credentials, and thereby, illegally accessing highly confidential and proprietary information belonging exclusively to

OpenEvidence, and misappropriating OpenEvidence's proprietary technology. As presently known to OpenEvidence, Pathway's unlawful efforts specifically include at least hundreds of cyber-attacks, including "prompt injection" hacking techniques, aimed at obtaining OpenEvidence's protected, confidential, and trade secret code and information, including OpenEvidence's System Prompt code.

This letter serves as formal notice that Pathway's actions are illegal under U.S. federal and state law. These actions specifically constitute trade secret misappropriation under federal law, violation of Mass. Gen. Laws ch. 93, theft, conversion, unfair competition (including under Mass. Gen. Laws ch. 93A), breach of contract, and violation of the Computer Fraud and Abuse Act, among other unlawful acts.

OpenEvidence demands that Pathway and its employees and agents immediately cease all improper access to OpenEvidence's portal and, by no later than December 23, 2024 at 5 pm ET:

1. Provide, in writing, detailed information about whether and to what extent Pathway is making use of information improperly obtained from OpenEvidence;

2. Provide written confirmation that Pathway has sequestered with an attorney or forensic neutral all documents and information, including outputs or code, obtained from OpenEvidence or referencing OpenEvidence, including without limitation any communications with investors, potential investors, customers or prospective customers; and

3. Make available for immediate digital forensic inspection Pathway's electronic devices and network, including all devices, including personal computers, laptop, and mobile devices associated with Louis Mullie, Hovhannes Karapetyan, Jonathan Hershon, Eric Yamga, Khudhur Mohammed, Vince Roy—individuals whose documents and files are likely to contain relevant information.

These initial demands are intended to preserve evidence and allow OpenEvidence to assess the breadth and extent of your wrongful actions and the appropriate remedies for such actions, including immediately ceasing to use any portion of OpenEvidence's proprietary information or technology platform on your website or in your product and service offerings.

Unless this matter is resolved unconditionally to OpenEvidence's satisfaction in the very near term, OpenEvidence will promptly commence legal action to protect its rights, including seeking equitable relief and compensation for ongoing economic and competitive harms.

With this correspondence, you also are undeniably on notice of OpenEvidence's claims. As a result, you are under a duty to preserve all potentially relevant evidence, including all emails, messages (including, but not limited to, all instant messages, messages and channels utilized via Slack or any other computer or electronic correspondence systems, SMS messages (including on personal devices); emails (including personal emails), Pathway code revision histories and change logs; and social media posts and direct messages), and other communications and records of communications, including but not limited to those associated with the following individuals:

- Louis Mullie
- Hovhannes Karapetyan
- Jonathan Hershon
- Eric Yamga
- Khudhur Mohammed
- Vince Roy

Should you fail to preserve all potentially relevant material, including that associated with the individuals above, that failure will constitute sanctionable spoliation under Federal Rule of Civil Procedure 37(e). Were this to happen, OpenEvidence would be entitled to, *inter alia*, an adverse inference, an award of attorneys' fees, and potentially case-termination sanctions. *See, e.g.*, *NuVasive, Inc. v. Day*, 2021 WL 9059745, at *8-9 (D. Mass. Aug. 23, 2021) (finding sanctionable spoliation based on deletion of text messages after duty to preserve evidence arose).

OpenEvidence reserves all rights.

Sincerely,

Robert D. Carroll

cc: John Egan, JEgan@goodwinlaw.com
L. Judson Welle, JWelle@goodwinlaw.com